KARAS & BRADFORD

325 S. MAIN STREET
Bel Air, MD 21014
410-836-0202

December 27, 2016

Via FedEX, Fax (410.576.6566) and Email (Idtheft@oag.state.md.us)

The Honorable Brian E. Frosh
Office of the Attorney General
Attn: Security Breach Notification
200 St. Paul Place
Baltimore, Maryland 21202

Re: Notification of Security Breach

Dear Attorney General Frosh:

I am writing to notify you that certain electronic files on computer systems belonging to Karas & Bradford ("K&B") were accessed by third-parties without authorization. Such access included electronic files on which resided personally identifiable information which K&B received on behalf of residents of Maryland in connection with a real estate transaction. Although there is no indication that any personal information was exfiltrated, it is possible that personal information of Maryland residents may have been viewed. Therefore, we are notifying affected residents as a cautionary measure in order to inform them of actions they may take to protect against any potential risks of fraud or other misuse of personal information.

On May 6, 2016, K&B learned that hackers had installed spyware on at least two of K&B's computers, and that the spyware gave the hackers the ability to see, read and copy documents and files on K&B's system, including documents and files which contain certain personally identifiable information of individuals to whom K&B provides services. After learning of the unauthorized access, K&B promptly engaged a cybersecurity forensics consultant and took steps to prevent further unauthorized access and remedy this situation, including contacting the FBI.

K&B is preparing to send written notification to all individuals who may be affected by this incident. A copy of the form of notification to Maryland residents is attached as Exhibit A.

To help protect affected individuals from the possibility of identity theft and/or fraud, K&B has offered a full-year of identity theft protection from AllClear ID, for each affected individual, at K&B's expense.

K&B takes information security very seriously and is committed to protecting the confidentiality of the information in its possession. K&B will continue to review its information security policies, procedures and practices, and will make improvements wherever appropriate in order to avoid a recurrence of this type of incident.

Please direct any questions to me either by phone 410-836-0202, or email tstevens@karasbradford.com.

Sincerely,

Charles E. Bradford

Enclosures

Exhibit A

Copy of Form of Notice to Affected Individuals

KARAS & BRADFORD

325 S. MAIN STREET
Bel Air, MD 21014
410-836-0202

December 22, 2016

[Name]
[Address]
[City, State, Zip Code]

Dear *[Name]*:

I am writing to notify you that certain electronic files on computer systems belonging to Karas & Bradford ("K&B") were accessed by third-parties without authorization. Such access included electronic files on which resided personally identifiable information you provided to K&B in connection with a real estate transaction to which you were a party. Although there is no indication that your personal information was exported, because our computer systems were accessed without authorization, it is possible that your personal information may have been viewed. Therefore, I am sending you this notice as a cautionary measure in order to inform you of actions you may take to protect yourself against any potential risks of fraud or other misuse of your personal information.

On May 6, 2016, K&B learned that hackers had installed spyware on at least two of K&B's computers, and that the spyware gave the hackers the ability to see, read and copy documents and files on K&B's system, including documents and files which contain certain personally identifiable information of individuals to whom K&B provides services. After learning of the unauthorized access, K&B promptly engaged a cybersecurity forensics consultant and took steps to prevent further unauthorized access and remedy this situation, including contacting the FBI.

Although at this time there is no evidence that personal information about you was accessed during this incident, in an abundance of caution, K&B believes that this notice is appropriate to ensure that you have the opportunity to protect yourself from any potential misuse of the information about which we are unaware. In addition, to help protect you from the possibility of identity theft and/or fraud as a result of this incident, K&B has engaged AllClear ID., an identity theft protection firm, to provide you with a full year of identity theft protection services at K&B's expense. For information about how to sign up for AllClear ID, please read the document attached to this letter. We encourage you to read the attached document carefully because it provides other important information intended to help you protect yourself from any potential misuse of your personal information.

K&B regrets that this incident occurred and is taking swift action to avoid a recurrence. Again, there is no indication that the individual gained unauthorized access to personal information about you. On behalf of our firm, I sincerely apologize for any inconvenience this incident may cause you, and thank you for your understanding and cooperation.

Sincerely,

Charles E. Bradford

UNAUTHORIZED ACCESS NOTIFICATION

Q: Why am I receiving this notification?

You are receiving this notification because of recent unauthorized access to K&B's computer systems that contained certain personal information of individuals to whom K&B provides services.

Q: What type of information is at risk?

The spyware installed on K&B's computer systems allowed hackers the ability to see, read and copy documents and files on K&B's systems, including documents and files which contained personal information such as:

(1) Name;
(2) Address;
(3) Phone number (s)
(4) Date of Birth
(5) Employment Information
(6) Monthly Income
(7) Information about assets and liabilities
(8) Ethnicity
(9) Sex
(10) Social Security Number;
(11) Driver's License Number;
(12) Credit Card Number
(13) Bank or Credit Union account information;
(14) Loan Origination Number
(15) Other information included in a Uniform Residential Loan Application (which may vary)

Q: Will K&B help me protect myself against the possibility that my information is misused?

As an added precaution, we have arranged to have AllClear ID protect your identity for 24 months at no cost to you. The following identity protection services start on the date of this notice and you can use them at any time during the next 24 months.

AllClear Identity Repair: This service is automatically available to you with no enrollment required. If a problem arises, simply call 1-877-676-0379 and a dedicated investigator will help recover financial losses, restore your credit and make sure your identity is returned to its proper condition.

AllClear Credit Monitoring: This service offers additional layers of protection including credit monitoring and a $1 million identity theft insurance policy. To use this service, you will need to provide your personal information to AllClear ID. You may sign up online at enroll.allclearid.com using the following redemption code: {Redemption_Code}.

K&B has also undertaken a full review of its information security policies, procedures and practices and is committed to making improvements wherever necessary to help protect all personal information stored on K&B's computer systems.

Q: Is there anything I can do to protect myself against the possibility that my information was accessed?

Yes. K&B recommends that you: (a) remain vigilant over the next twelve to twenty-four months; (b) immediately report any suspicious activity or incidents (including suspected identity theft) both to K&B and the bank or credit union from which you obtained your mortgage or home equity line; and (c) take the following measures to protect yourself from the possibility of fraud and identity theft.

You should monitor your credit card and bank or credit union account statements. You should also obtain free credit reports and monitor them for unexplained, suspicious or unauthorized activity. You may obtain a copy of your credit report once per year, free of charge, whether or not you suspect any unauthorized activity on your account, by contacting each of the nationwide consumer credit reporting agencies identified below, or by visiting www.annualcreditreport.com. You may obtain information about additional protections, such as fraud alerts and security freezes, from each of the three credit reporting agencies shown below.

Equifax
(888) 766-0008
P.O. Box 740256
Atlanta, GA 30374
www.equifax.com

Experian
(888) 397-3742
P.O. Box 2104
Allen, TX 75013
www.experian.com

TransUnion
(800) 680-7289
P.O. Box 6790
Fullerton, CA 92834
www.transunion.com

The Federal Trade Commission (FTC) recommends that you check your credit reports periodically to help you spot problems and address them quickly. If a report shows accounts you did not open, inquiries from creditors that you did not initiate, personal information, such as a home address, that is inaccurate, or other information you do not understand, contact one of the credit reporting agencies immediately. In addition, if you find suspicious activity on your credit reports or have reason to believe your personal information is being misused, authorities generally recommend that you take two additional steps: First, call your local law enforcement agency and file a police report and get a copy of the police report because many creditors want the information it contains to absolve you of any fraudulent charges. Second, file a complaint with the FTC, which will be added to the FTC's Identity Theft Data Clearinghouse, where it will be accessible to law enforcement agencies for their investigations.

You can file a complaint or obtain additional information about preventing identity theft from the Federal Trade Commission:

Federal Trade Commission
600 Pennsylvania Avenue, NW
Washington, DC 20580
www.consumer.gov/idtheft
Toll free: (877) 438-4338

Q: How do I request a security freeze?

Following is general information about how to request a security freeze from the three credit reporting agencies. While we believe this information is accurate, you should contact each agency for the most accurate and up-to-date information.

A security freeze prohibits a credit reporting agency from releasing any information from a consumer's credit report without written authorization. However, please be aware that placing a security freeze on your credit report may delay, interfere with, or prevent the timely approval of

any requests you make for new loans, credit mortgages, employment, housing or other services. In some states, if you have been a victim of identity theft, and you provide the credit reporting agency with a valid police report, the agency cannot charge you to place, lift or remove a security freeze. In all other cases, a credit reporting agency may charge you up to $10.00 each to place, temporarily lift, or permanently remove a security freeze.

To place a security freeze on your credit report, you must send a written request to **each** of the three major consumer reporting agencies: Equifax (www.equifax.com); Experian (www.experian.com); and TransUnion (www.transunion.com) by regular, certified or overnight mail at the addresses below:

Equifax Security Freeze P.O. Box 105788 Atlanta, GA 30348 https://www.freeze.equifax.com	**Experian Security Freeze** P.O. Box 9554 Allen, TX 75013 www.experian.com/freeze	**TransUnion Security Freeze & Fraud Victim Assistance Dept.** P.O. Box 6790 Fullerton, CA 92834 https://freeze.transunion.com

In order to request a security freeze, you will need to provide the following information:

- Your full name (including middle initial as well as Jr., Sr., II, III, etc.);
- Social Security Number;
- Date of birth;
- If you have moved in the past five (5) years, provide the addresses where you have lived over the prior five years;
- Proof of current address such as a current utility bill or telephone bill;
- A legible photocopy of a government issued identification card (state driver's license or ID card, military identification, etc.);
- If you are a victim of identity theft, include a copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft;
- If you are not a victim of identity theft, include payment by check, money order, or credit card (Visa, MasterCard, American Express or Discover only). Do not send cash through the mail.

The credit reporting agencies have three (3) business days after receiving your request to place a security freeze on your credit report. The credit agencies must also send written confirmation to you within five (5) business days and provide you with a unique personal identification number (PIN) or password, or both, that can be used by you to authorize the removal or lifting of the security freeze.

To lift the security freeze in order to allow a specific entity or individual access to your credit report, you must call or send a written request to the credit reporting agencies by mail and include proper identification (name, address, and social security number) **and** the PIN number or password provided to you when you placed the security freeze as well as the identities of those entities or individuals you would like to receive your credit report or the specific period of time you want the credit report available. The credit reporting agencies have three (3) business days after receiving your request to lift the security freeze for those identified entities or for the specified period of time.

To remove the security freeze, you must send a written request to each of the three credit bureaus by mail and include proper identification (name, address, and social security number) **and** the PIN number or password provided to you when you placed the security freeze. The credit bureaus

have three (3) business days after receiving your request to remove the security freeze.

Q: Are there state resources that can assist me in protecting my identity?

Yes. K&B recommends that you utilize these resources to protect yourself from the possibility of fraud and identity theft.

For Maryland residents, the MD Office of the Attorney General can provide you with additional information about steps you can take to avoid identity theft and may be contacted at:

Maryland Office of the Attorney General
Consumer Protection Division
200 Saint Paul Place
Baltimore, Maryland 21202
Toll free: (888) 743-0023
http://www.marylandattorneygeneral.gov/Pages/IdentityTheft/default.aspx

Q: Who can I contact at K&B for additional information?

To answer any question or address any concerns you may have, please contact us by any of the following methods:

email: **tstevens@karasbradford.com**
phone: **410-836-0202 x3**
mail: **325 S. Main Street, Bel Air, MD 21014**